SECURITY AND SCIENCE AT LAWRENCE LIVERMORE NATIONAL LABORATORY

Hearing of the U.S. Senate Select Committee on Intelligence
July 14, 1999

C. Bruce Tarter, Director
Lawrence Livermore National Laboratory
University of California

OPENING REMARKS

Mr. Chairman and members of the committee, I am the Director of the Lawrence Livermore National Laboratory (LLNL). Thank you for the opportunity to appear before you today. I intend to discuss very important issues concerning how we apply the very best in science and technology to accomplish our national security mission and, at the same time, provide security and protect nuclear secrets.

Our Laboratory was founded in 1952 as a nuclear weapons laboratory, and national security continues to be our central mission. Livermore is a principal participant in the Department of Energy's Stockpile Stewardship Program and heavily involved in programs to prevent the proliferation of weapons of mass destruction. We also apply our core technologies to research and development in related areas of energy, environment, and bioscience as well as industrial applications.

Security and science are both central to Livermore's purpose and its operations. They are tightly tied together throughout our programs. Through the Stockpile Stewardship Program, we further national security by applying advances in science and technology to maintain the nation's nuclear stockpile in the absence of nuclear testing. With less than 2% of the world's research and development being conducted at DOE national laboratories, many of the scientific advances that we adapt and apply to specific national security problems are made elsewhere. Hence, we depend on interactions with the broad science and technology community to be cognizant of major advances and to acquire special expertise needed to accomplish mission goals. By necessity, we work extensively with U.S. universities and industry, which include significant numbers of non-U.S. citizens, and considerable expertise in some technical areas exists abroad. We also engage foreign nationals as part of our national security mission through participation in international efforts to prevent the spread of nuclear weapons, materials, and know-how. Accomplishing our mission depends critically on science and technology interactions within DOE, throughout the United States, and worldwide, but we must manage our interactions in a way that protects national security interests.

When we interact with others—including foreign nationals—whether on site or off site, it is mandatory that we protect sensitive information. An extensive security apparatus is in place at our Laboratory, and we continually make adjustments and upgrades to address new threats and concerns. We take strong positive action on counterintelligence issues, whether they are anticipated or identified by us, by others, or raised by executive or departmental orders. Today, I would like to discuss this triad of security—physical, cyber, and counterintelligence—and its application at Livermore. Then I will elaborate on the importance to the Laboratory's mission of broad participation in the international science community and comment on our "culture."

PHYSICAL SECURITY AT LIVERMORE

Livermore's security construct is based on a series of defensive layers—a graded approach that provides increasing barriers that correspond to the increasing security value of critical Laboratory assets.

Clearances, badging, and background checks on Laboratory employees (including subcontractors) constitute a first line of defense. Those people with access to the highest levels of classified assets undergo background investigations associated with DOE Q and L clearances and sensitive compartmented information (SCI). Reinvestigations are scheduled automatically at five-year intervals or as needed on a for-cause basis.

Livermore uses a defense-in-depth approach to physical barriers—fences, doors, repositories, and vaults. The Laboratory's outer perimeter fence provides the basic physical protection to U.S. government property. Additional protection is provided for "limited" areas where classified assets are present. The level of clearance required to transit these areas is also higher. Classified parts and materials are provided additional physical protection and access control. Significant quantities of special nuclear material receive the highest level of protection, with vault-like physical protection as well as aggressive armed defense and response capabilities.

At each physical barrier (e.g., fence, building, vault), there are various levels of access control. Security officers check badges and in more restricted areas, they check people against specific access lists; at unmanned security portals, badges are checked against access lists. Need-to-know is required, in addition to the appropriate clearance, before an individual is allowed access to classified assets.

The Laboratory employs security officers who are fully trained and accredited. The level of training varies with the assignment (defensive, offensive, or special response). We currently have over 40 offensively trained officers in our Special Response Team and have an additional 15 or so beginning training next month. Training is extensive and performance-based. The security force undergoes regular performance tests, self-assessments, DOE surveillance, and inspections.

Physical security is designed into new facilities and facility modifications. Detection systems are continuously monitored and routinely tested. The Laboratory's security system is prepared for armed response to all unauthorized intrusions.

At Livermore, we believe our Special Nuclear Materials (SNM) and sensitive and classified information are secure today. However, during the last year, the Laboratory received a "marginal" rating in safeguards and security, and we have already addressed or are aggressively moving forward to correct all identified issues before the end of the year. A significant issue involved our inability to meet SNM inventory requirements at a time when the Plutonium Facility was shut down to address safety concerns, preventing monitoring and measurements. Now that safety concerns have been addressed and the facility reopened, we have resumed all special nuclear material measurements and inventory monitoring and we believe we are now compliant with DOE requirements.

A second concern raised in reviews was the lack of a documented ability to assure protection of SNM. We are currently conducting detailed simulations and performance tests and adjusting our protection strategy to counter any foreseeable threat. We are doing this in conjunction with the DOE Office of Security Evaluations, and we are also employing external consultants and advisors. This approach, along with the additional Special

Response Team members being trained, has us on a path to correct physical security issues before the end of the year. We have taken interim steps to assure high-confidence protection until the longer-term measures are in place.

A third concern involved the protection of classified matter. In particular, some parts awaiting processing or use were in storage areas that needed additional alarms within the limited-access portion of the Laboratory. We are moving to install the additional alarms; in the interim, security officers are providing additional protection.

In summary, we have high confidence in our Safeguards and Security programs and in the security of our critical assets. We have implemented technical and procedural enhancements to strengthen our physical security, remedied material control and accounting deficiencies, and revised our strategy to protect nuclear material at the Laboratory (including the deployment of a Special Response Team).

CYBER SECURITY AT LIVERMORE

Cyber or computer security is a critical element of Livermore's overall security construct. The Laboratory has both classified computer networks and unclassified computer networks. The two are separate and are not connected. We also have numerous stand-alone computer systems and local area networks in both classified and unclassified areas. There are no connections from Livermore's classified computers to the outside world except through NSA-approved encryption.

In addition to physical barriers between the unclassified and classified computing environments at Livermore, there are need-to-know barriers within the classified computer systems. Access to a classified computing network does not grant users access to all the information in that network. The same need-to-know requirements that apply to verbally communicated information and documents also apply to computer-stored information.

Recent concerns about espionage involving computer-based information and codes spurred a thorough reassessment of computer security at our Laboratory, including threat awareness and training. We are vigorously supporting and helping to develop the Secretary of Energy's cyber security initiative and are contributing to his INFOSEC planning on a number of fronts.

On April 2, 1999, the Secretary of Energy called for a stand-down of all classified computing at the three DOE national security laboratories. At Livermore, we went even further and shut down all classified computing, all co-located unclassified computing, and all unclassified supercomputing. The stand-down was the first step of a Tri-Lab INFOSEC Action Plan that has been developed and approved by Secretary Richardson. The plan consists of nine action items with specific scheduled milestones. We have met all agreed-to milestones to date. We will continue working with the DOE Office of the Chief Information Officer (CIO) to fully implement the Tri-Lab INFOSEC Action Plan and further enhance cyber security at the Laboratory.

In addition, on June 21-22, 1999, we conducted a two-day-long Security Immersion Program at Livermore to accelerate the security initiatives launched by Secretary Richardson in April. Supervisors were instructed to ensure that all Laboratory employees complete the program, which was directed toward five objectives identified by the Secretary to strengthen security at the laboratories, assessing security issues in individual work areas, and applying what has been learned to each individual's workplace.

We have taken dramatic steps to focus the attention of all Laboratory employees on the threat of foreign intelligence sources as related to cyber security. All employees (including those who do not normally use computers but could have need or access in the future) received special computer security training. We also trained subcontract employees and consultants. All computing was discontinued until training was complete for all employees on site. Employees who were on travel or leave were trained immediately upon their return. In addition, we have since expanded our on-going computer security training and threat awareness training for all Laboratory personnel using classified computers. This training is unclassified and accessible via a Web site to make it readily available to our employees and easy to update.

Every computer work area and environment at Livermore was evaluated and changes were made as necessary to ensure that the Laboratory's classified and sensitive computing meet the highest standards of information security. In particular:

- We have taken measures to preclude the transfer of information from classified to unclassified computers in a single work area by the use of removable media.

- We have instituted two-person controls over the authorized transfer of unclassified information from classified computers to unclassified computers.

- Until a more permanent security fix is in place, since April 2, 1999, we have temporarily disabled the file interchange system on the classified supercomputer so that it is impossible to transfer files from the classified supercomputers or the archives to an unclassified computer.

- We have begun to scan outgoing unclassified e-mail as well as computer files for possible sensitive or classified information. To date, we have scanned over 4 million files in our effort to locate classified material in unclassified computer files. No issues have arisen.

- We have strong need-to-know controls on our classified network; yet, we are investigating ways to provide an even greater level of protection. We are also studying how to apply these same concepts to the unclassified systems to provide better protection to unclassified sensitive information.

In addition, I have also created a Computer Security Policy Board comprised of senior managers to both develop policies and advise me on matters related to unclassified computer security. (Classified computer security policy is defined by DOE Orders.)

On our unclassified computing network, we are improving the way we protect unclassified sensitive information. Some information must be available worldwide, but other information must be protected for privacy, proprietary, or export control reasons. We are implementing additional "firewalls" within our unclassified network to separate fully accessible information from unclassified sensitive information. For several years, Livermore has had an on-going program to annually scan/audit a sub-set of its unclassified computer systems for security vulnerabilities. We have changed this policy so that now all unclassified computer systems must be scanned at least once a year and that appropriate corrections/fixes to detected vulnerabilities must be undertaken immediately.

The Laboratory has long had a policy of monitoring users accessing our computer resources via the Internet. We have now expanded our monitoring to cover all dial in access to Livermore computers. Specifically, any Foreign Nationals (FNs) with dial-in capabilities are monitored. However, any FN granted access to unclassified computer resources must first have a programmatic justification of need by the sponsoring Laboratory program and

an approved security plan on record for each FN. In addition, the Laboratory required that all FNs with access to computer resources had to be recertified by June 30, 1999. No one was "grandfathered" in under our process and those not recertified are being denied access to the computer resources. Certification refers to having a programmatic justification and a security plan in place. Livermore will require that all FNs granted access to Laboratory computer resources must be processed through the Foreign Visits and Assignments Office. This will ensure that any FN with access to Laboratory computer resources will have received the proper approval and that their access to computer resources is being monitored.

Finally, our Laboratory is working with personnel at Sandia, Los Alamos, and DOE to develop a "best in practice" plan for cyber security. So far, we have completed a benchmarking of several organizations inside and outside of the government to determine what others are doing to protect information from both outsiders and insiders. This planning activity has an oversight board that is currently being staffed with cyber security professionals from industry along with the CIOs from the three laboratories.

Our approach to cyber security goes beyond addressing vulnerabilities or problems that we identify or that are brought to our attention. We are using this cyber security upgrade as an opportunity to apply our multi-disciplinary approach to science and technology to become a model for cyber security. Leading-edge cyber security is vital to our programmatic missions and is an area where we can leverage our expertise to enhance national security in the broadest sense.

LIVERMORE'S COUNTERINTELLIGENCE PROGRAM

Livermore's formal counterintelligence program (Security Awareness for Employees, or SAFE) was established in January 1986 in response to a Presidential Decision Directive dated November 1, 1985, that required all U.S. government agencies to establish their own counterintelligence programs. The impetus for the directive was a number of cases in the 1980s of U.S. citizens spying against the United States. (Prior to this time, Livermore addressed counterintelligence concerns through cooperation with the local FBI office, including joint work of mutual benefit and regular discussions on how to reduce the threat of espionage.)

SAFE's purpose is to identify and counter foreign intelligence threats against Laboratory personnel, information, and technologies. Central to this effort is employee awareness about counterintelligence issues. SAFE provides briefings and debriefings for personnel who host foreign visitors or travel abroad as well as presentations on espionage-related topics by guest speakers from the U.S. intelligence community. These activities help employees recognize if they are the subject of espionage recruitment or information collection efforts by foreign agents and teach them what to do in such a situation. SAFE also provides a consistent way of checking the backgrounds of all foreign contacts.

Livermore notifies the U.S. Department of Energy (DOE) Office of Counterintelligence of all proposed visits or assignments of sensitive country foreign nationals to the Laboratory, so that that office can request necessary background checks. SAFE also notifies the local FBI field office of proposed visits by foreign nationals from Russia or China. In addition to the pre-travel and pre-visit briefings required by DOE Orders, SAFE also debriefs Laboratory travelers and hosts at the conclusion of their foreign travel or foreign national visit. The information gathered from these debriefings is shared with the U.S. intelligence community, providing valuable input regarding the continually evolving

espionage threat as well as feedback on the effectiveness of SAFE's counterintelligence efforts.

History of the SAFE Program

During SAFE's early years, we took a number of steps to align our counterintelligence program closely to the FBI model. By the mid-1990s, SAFE was functioning effectively at LLNL and was well integrated into the U.S. counterintelligence community.

In the early 1990s, in response to the Laboratory's growing number of foreign interactions, particularly lab-to-lab programs, SAFE hired several analysts from the U.S. counterintelligence community. In 1992 a former CIA foreign intelligence analyst and Russia expert was hired, and in 1993 a former FBI Supervisory Special Agent and China expert was brought in to manage the SAFE program. Another former FBI China expert was hired in 1994, and a former FBI Middle East and counterterrorism expert was brought on board in 1997. In May 1999, another former FBI China expert was added to SAFE's staff.

Over the years, SAFE has increased the depth and specificity of its briefings for Laboratory employees embarking on foreign travel or hosting foreign visitors or assignees. SAFE reviews the proposed travel or visit, taking into consideration such factors as the foreign country involved, the length of stay, the subject matter to be discussed or studied, the specific facilities or areas to be visited (in the foreign country or at Livermore), and applicable U.S. or foreign government restrictions. If necessary, SAFE works with the traveler or host to modify the travel or visit or deny it.

In August 1996, we took another step to augment counterintelligence related to foreign travel and foreign national visitors. Our Proliferation Prevention and Arms Control Program took on the technical review of all requests for travel to sensitive countries by Laboratory employees and all visits and assignments to the Laboratory by foreign nationals from the former Soviet Union, Middle East, Eastern Europe, South Asia, and the Pacific Rim. These reviews focus on the technical content of the proposed travel or visit as it relates to the likely benefits to the foreign country's weapons programs and the concomitant risks posed to U.S. national security.

Response to Curtis Tasking

In November 1996, DOE Deputy Secretary Curtis met with the Directors of the Los Alamos, Lawrence Livermore, Sandia, Oak Ridge, and Pacific Northwest National Laboratories to address the foreign visits and assignments programs at those laboratories. Three taskings specific to the laboratories resulted from this meeting: conducting foreign intelligence threat assessments at each lab, developing a new database to track foreign visits and assignments, and updating the sensitive unclassified topics list.

At Livermore, a Foreign Interactions Day was held in December 1996 in which senior Laboratory managers laid out plans for meeting these Curtis initiatives. Livermore's self-assessment of the threat posed by foreign intelligence collection efforts was launched immediately. Our threat assessment was conducted with assistance from DOE's counterintelligence program (NN-30), and a report documenting our findings was provided to DOE in April 1997.

In March 1997, Livermore hosted a DOE-wide workshop to design an improved database for tracking foreign visits and assignments. The initial idea was for a system that could be used by all the DOE laboratories. In April, we submitted a proposal for a DOE-

wide database to track foreign visits and assignments. When DOE declined to adopt a single database design for use by all the laboratories, we went on to design, develop, test, and implement the Visitor Tracking System for use at Livermore. As of May 3, 1999, this system is functional across the Laboratory. Information on each foreign visit and assignment is entered into the system as part of the review and approval process. The database automatically captures numerous pieces of information about each visit and assignment and can provide statistics as needed for periodic reviews and for refined management of the foreign visit and assignment program.

The technical content of proposed foreign visits and assignments is evaluated against a list of sensitive unclassified topics. The purpose of this list is to identify those unclassified topics and technologies that potentially include sensitive information that can be disseminated only after careful review of the specific topic and recipient. Sensitive information is information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or federal government interests. Defining sensitive unclassified topics and technologies is a difficult and complex task. Such a list must be used as an indicator that careful attention is required, not as a mechanism for automatic decisions on access. Sound technical judgment must be applied, using the list as guidance, to make a reasoned weighing of proliferation and national security concerns vis a vis the value of scientific interactions.

Livermore's sensitive unclassified topics list, initially drawn up in 1995, is available for reference on the Laboratory's internal web site. Although no DOE Headquarters-led effort for a department-wide update of the sensitive unclassified topics list materialized after the November 1996 Curtis meeting, we have had an ongoing effort at Livermore to keep current our critical and sensitive information list (CSIL; a classified compilation). This list is updated annually through the Laboratory's Operational Security (OPSEC) committee. Most recently, in early April 1999, we convened a team of senior Laboratory managers and scientists to rethink the sensitive unclassified technologies list. This group coordinated its efforts with similar teams at Los Alamos and Sandia. Livermore's draft list of sensitive unclassified technical information was completed April 30, 1999, and has been sent to the Director of DOE's Office of Counterintelligence for review and comment.

We have taken other counterintelligence measures related to but independent of the Curtis initiatives. We made a number of changes to our foreign visits and assignments program to provide better control and tracking, including a more restrictive badging policy for foreign visitors (effective March 1997). We now include several senior Laboratory managers in the review and approval process for foreign visits and assignments, which helps give Laboratory management a better understanding of the counterintelligence concerns surrounding these visits and assignments.

In early 1998, we drafted an export control guide to assist Laboratory participants in the DOE Materials Protection, Control, and Accounting (MPC&A) program and other activities involving collaborations with Russian and former Soviet scientists. Later that year, we revised that guide and incorporated export control guidance from other programs to produce a comprehensive Laboratory-wide guide to export control. We coordinated our effort with our counterparts at Los Alamos and Sandia to ensure that all three laboratories are operating under consistent export control guidance. This document was distributed to Laboratory employees in May 1999, and it is also accessible electronically on our internal web site.

Response to PDD 61

Presidential Decision Directive (PDD) 61, issued in February 1998, ordered the DOE to establish a stronger counterintelligence program. In February 1999, the DOE issued its plan for implementing PDD 61. At Livermore, we are moving ahead vigorously with many actions in response to the recommendations in the implementation plan that affect the Laboratory.

The plan's counterintelligence recommendations fall into several broad categories: structure and staffing of the laboratories' counterintelligence programs, liaison with the FBI, counterintelligence and security briefings, insider threats, and foreign national contacts.

The plan calls for counterintelligence programs, within the DOE and at the laboratories, to be separated from their organizations' security departments. Livermore's counterintelligence (SAFE) program meets this recommendation. When it was first established, the SAFE program reported to the Director's Office. Since 1995, the SAFE program has resided in the Nonproliferation, Arms Control, and International Security (NAI) Directorate. The Associate Director for NAI is the Laboratory's Senior Intelligence Officer, and the SAFE program manager has direct access to both the NAI Associate Director and the Laboratory Director.

The plan also calls for the laboratories' counterintelligence programs to be staffed with and managed by experienced counterintelligence personnel and intelligence analysts. Since its inception, our SAFE program has been managed by an experienced former employee of the U.S. intelligence community. SAFE's first program manager was a former CIA counterintelligence specialist. SAFE's current manager is a former FBI Supervisory Special Agent. He is assisted by three former FBI agents and one former CIA case officer. In addition, SAFE is a functional part of the Laboratory's Field Intelligence Element (FIE). SAFE draws heavily and frequently on the Laboratory's intelligence analysts and their expertise in foreign weapons programs; SAFE also employs an analyst (half-time) devoted strictly to counterintelligence issues.

Since the 1970s, our Laboratory has engaged in formal interaction with the FBI on counterintelligence matters. Early in 1996, at our initiative, the FBI placed a liaison agent in the SAFE program. Since the late 1980s, FBI Special Agents in Charge from the San Francisco division have visited Livermore for exchanges of information with senior Laboratory management; the most recent visit took place in March 1999, when Livermore hosted Mr. Bruce Gebhardt, the current Special Agent in Charge.

The DOE plan mandates that counterintelligence and security briefings be tailored to reach all segments of the DOE community. Livermore's counterintelligence and security programs produce high-quality focused briefings for all Laboratory personnel. Livermore employees receive periodic security and counterintelligence awareness briefings. All employees, regardless of clearance level, are required to take an annual security and counterintelligence refresher briefing. SAFE sponsors several counterintelligence awareness briefings each year for Laboratory employees, often by speakers from the U.S. intelligence community. In addition, SAFE gives numerous counterintelligence presentations to groups of employees; many of the unclassified presentations are given to uncleared personnel.

In addressing the need to protect against insider threats, the plan's recommendations focus primarily on the need to expand the DOE's current polygraph program and for the laboratories to establish Personnel Evaluation Boards. At present, Livermore does not have

a Personnel Evaluation Board as such. We do however have a formalized process for reviewing cases involving employees being considered for adverse employment actions. The Laboratory's Staff Relations Office oversees this review and evaluation process, working initially with managers in the affected employee's department. A review panel of selected Laboratory managers is convened, and representatives of Human Resources, Office of General Counsel, and Personnel Security are brought in as relevant to the specific case. The panel recommends the action to be taken by the Laboratory, based on numerous criteria present in the matter under review. The SAFE program manager is called by the review panel for consultation should panel members become concerned that actions by an employee are suggestive of espionage activity.

The plan also calls for action regarding foreign national contacts at the laboratories. In December 1998, we completely revised our review and approval process for foreign visits and assignments, particularly with regard to sensitive-country foreign nationals. This layered review involves counterintelligence, security, export control, and nonproliferation as well as several senior Laboratory managers. A sensitive-country foreign visit or assignment is not approved until a background (indices) check has been completed. Livermore's Proliferation Prevention and Arms Control Program also evaluates each proposed foreign visit or assignment against U.S. foreign policy priorities.

In addition to the Visitor Tracking System mentioned above, we also initiated a Foreign National Database Project, under the direction of the SAFE program, to capture all pertinent data on foreign visits and assignments to Livermore that occurred between 1994 and 1998. As part of this effort, each Laboratory directorate is developing its own list of sensitive topics that reflects the technical subject matter that was (or could be in the future) relevant to those foreign visits and assignments.

For many years, Livermore has provided guidance to employees to report any close and continuing contact with foreign nationals from sensitive countries. Guidance from our counterintelligence and security programs is based on requirements in the DOE foreign visits and assignments order as well as other DOE security and counterintelligence orders. This reporting requirement is articulated to Laboratory employees in annual counterintelligence awareness briefings as well as in oral and written counterintelligence briefings to Laboratory hosts of sensitive-country foreign national visitors and assignees. We also provide counterintelligence briefings to employees traveling to sensitive countries. Our goal and practice is to brief and debrief all Livermore employees who serve as hosts to sensitive-country foreign visitors and assignees and all employees who travel to sensitive countries.

SCIENCE, THE LABORATORY, AND ITS CULTURE

Livermore is an integral part of the DOE Stockpile Stewardship Program for ensuring that the nation's nuclear weapons remain safe, secure, and reliable. Livermore also has a primary role in the DOE's mission to prevent the spread and use of nuclear weapons, as well as other weapons of mass destruction (WMD). The challenges posed by these extraordinarily demanding responsibilities can only be met if the Laboratory research and development efforts, as reflected in its workforce and research facilities, are at the cutting edge of science and technology.

World-class science and technology is not possible without being active in the broad scientific community. With less than 2% of the world's research and development being conducted at DOE national laboratories, the laboratories depend on external interactions to be cognizant of major advances and to acquire special expertise needed to accomplish

mission goals. By necessity, we work extensively with U.S. universities and industry, which include significant numbers of non-U.S. citizens, and considerable expertise in some technical areas exists abroad. Our external interactions, which vary in extent depending on the research area, include travel, conferences, visits to the Laboratory by both citizens and foreign nationals, and occasionally more extensive technical discussions and participation in specific research projects by people outside the Laboratory. Livermore scientists also engage foreign nationals as part of its national security mission through participation in international efforts to prevent the spread of nuclear weapons, materials, and know-how.

A consequence of Livermore's multidisciplinary capabilities is that the Laboratory has multiprogram responsibilities. Livermore focuses applies its core capabilities and special attention on the enduring missions of DOE in energy, environment, bioscience, and science and technology. Rather than detracting from the Laboratory's national security work, these other activities strengthen it. They lead to cross-fertilization of ideas and spin-back to the national security mission; they provide additional support to the technology base that is needed for national security; and they draw top notch talent to the Laboratory that have had no prior exposure to the existing opportunities and challenges in stockpile stewardship or nonproliferation. Our non-national-security research efforts, which are almost always unclassified, build upon Livermore's technical leadership in selected research areas and involve foreign interactions.

International Interactions—Benefits to Stockpile Stewardship

The Stockpile Stewardship Program for maintaining the nuclear weapons stockpile is a technically ambitious program whose success depends on adaptation and application of the best science and technology has to offer to nuclear-weapons specific issues. The program, often referred to as "science-based" stockpile stewardship, depends on bringing into operation vastly improved scientific capabilities that are, in many key areas, the best in the world. In the absence of nuclear testing, stockpile performance is to be ensured by using laboratory experiments and computer modeling to achieve a much more sophisticated understanding of underlying physics and engineering issues. Acquisition of the needed capabilities requires a broad range of interactions with industry, universities, and other laboratories—and, invariably foreign nationals.

The Stockpile Stewardship Program requires state of the art science and technology to meet the challenges that lie ahead as U.S. nuclear weapons continue to age. The demands on the program are in many areas: lasers, computers, materials science, and engineering to name but a few. The Laboratory would not able to acquire and effectively use leading-edge scientific capabilities it needs without broad interactions with the global technical community. Within U.S. universities, for example, nearly half of the students enrolled in physics graduate programs are non-U.S. citizens. In many areas, we depend on foreign nationals to provide cutting-edge expertise.

An important component of stockpile stewardship is the Accelerated Strategic Computing Initiative (ASCI) to dramatically advance capabilities to computationally simulate the performance of an aging stockpile and the conditions affecting weapon safety. The initiative entails major partnerships among the computer industry, universities and researchers worldwide that are at the forefront of the "science" of scientific computing, and the DOE national security laboratories. In addition to our numerous academic collaborations to accelerate research in massively-parallel computing, several of the leading-edge techniques that are being applied to benefit stockpile stewardship are the products of foreign nationals working on unclassified projects at the Laboratory. A citizen of

Switzerland is developing state-of-the-art computational physics and molecular dynamics models that help Laboratory scientists better understand the properties of materials important to stockpile stewardship. A citizen of Bulgaria is providing world-class expertise on solving partial differential equations on massively parallel computers. His advances have many applications in computational materials science and fluid dynamics. Citizens of Canada and Spain are among other researchers making major strides in computer science to the benefit of Laboratory scientists working stockpile stewardship issues.

Foreign-national interactions are also providing essential support to the construction of the National Ignition Facility (NIF), a 192-beam laser that will be a cornerstone of the Stockpile Stewardship Program. It will be the only facility capable of experiments to study the thermonuclear properties of primaries and secondaries in nuclear weapons. The NIF project is a major partnership with U.S. industry and includes participation by the British and French. An enabling technology for NIF is a process, invented by a citizen of Russia now working at the Laboratory, for rapidly growing large, flawless KDP (potassium dihydrogen phosphate) crystals for NIF's laser systems. Other important technology advances supportive of the NIF and ICF programs are the work of Laboratory employees that are citizens of Belgium, Canada, and the United Kingdom.

International Interactions—A Necessary Part of the Nonproliferation Mission

The U.S. government sponsors a variety of national security programs at Livermore that require foreign interactions, sometimes with citizens of sensitive countries. Many of these activities, which are integral to Livermore's nonproliferation and arms control mission, specifically require nuclear weapons expertise present at the DOE national security laboratories. Furthermore, in contrast to the Cold War years when almost all of the technologies developed at Livermore were solely for U.S. use, many of our new technologies and tools are designed for use in a multilateral security environment.

Interactions range from confidence-building discussions to cooperative research projects on unclassified subjects to joint development of treaty-related procedures and technologies. These activities necessitate attendance at professional meetings also attended by U.S. and foreign scientists, travel by Livermore scientists to foreign institutes, and visits by foreign nationals to the Laboratory. Some principal project areas include:

Protection and Control of Nuclear Materials. Livermore is contributing to U.S. efforts to improve the protection and control of weapons-usable nuclear materials in Russia and worldwide. Livermore participates in the DOE's Material Protection, Control, and Accounting (MPC&A) program and has the lead at five MPC&A sites in Russia, including Chelyabinsk-70 (one of the former Soviet nuclear weapons design laboratories). In addition, we work with the Russian Navy and the Murmansk Shipping Company to improve the protection of fresh, highly enriched reactor fuel for their nuclear-powered vessels; the activities involve direct interactions with the Russian Ministry of Defense.

Livermore is also a principal participant in the U.S.–Russian Second Line of Defense program, designed to curtail the illicit transport of items of nuclear proliferation concern from Russia. We are working with Russian Customs to equip border crossings with radiation detection equipment and to help train customs officials. In addition, we are working with Russian institutes to developed improved techniques and instruments for detecting smuggled fissile materials.

Preventing the Spread of WMD Expertise. We participate in several programs to assist the weapons institutes and scientists in Russia and the other newly independent states

(NIS) in the conversion to civilian and commercial applications of their weapons-related technologies and expertise. Through the International Science and Technology Center (ISTC) and the Science and Technology Center of Ukraine, more than 900 projects have supported work involving over 29,000 scientists in the former Soviet Union. Livermore is currently collaborating on more than 50 projects. In the Initiatives for Proliferation Prevention (IPP) program, collaborative projects among DOE's national laboratories, U.S. industry partners, and 170 NIS institutes are aimed at developing commercially viable applications or adaptations of defense-related technologies. Livermore collaborates on 50 such projects, which support nearly 1000 former Soviet weapons scientists. Finally, Livermore will be working with City of Snezhinsk (home of Chelyabinsk-70) as part of the Nuclear Cities Initiative (NCI). The NCI is a new nonproliferation effort in which the DOE national security laboratories will work with Minatom to help the "closed cities" become more self-sustaining through conversion to nonmilitary commercial applications of their weapons-related technologies, expertise, and facilities.

Dismantlement and Disposition. Livermore is heavily involved in a wide range of warhead dismantlement and fissile material activities, including dismantlement transparency, highly enriched uranium (HEU) purchase transparency, and excess fissile material storage and disposition. Through several DOE programs we work with our Russian counterparts to develop mutually acceptable methods of verifying the presence of weapons-grade fissile material without revealing sensitive or classified information. Such methods are required for implementation of the Plutonium Production Reactor Agreement and for dismantlement transparency measures. Candidate monitoring instruments have been developed by Livermore scientists and demonstrated to the Russians and the International Atomic Energy Agency (IAEA) at Livermore's Superblock and in Russia.

Livermore also has the technical lead for the Joint U.S.–Russian plutonium disposition activities to stabilize, immobilize, and geologically dispose of excess Russian weapons-origin plutonium. Working with the Russians, a strategy has been developed for industrial-scale immobilization of Russian impure excess weapons-plutonium-containing materials at one or more of the three plutonium processing sites in Russia by the year 2004.

Export Control. Control of exports that could lead to WMD proliferation is one of the cornerstones of U.S. nonproliferation policy, and Livermore works to promote effective export control internationally. Through the DOE, Livermore directly supports U.S. activities in the thirty-five-member Nuclear Suppliers Group and is active in international export control assistance programs. For example, this past year, we organized several export control workshops with the Russians.

CTBT Technical Support. Livermore scientists engage in international activities related to the Comprehensive Test Ban Treaty (CTBT). A Livermore researcher is the U.S. point of contact for on-site inspection (OSI) issues at the CTBT Preparatory Commission in Vienna. This past year, he led the international development of the OSI concept of operations, clearing the way for work on the development of the OSI operations manual. We also conducted a joint OSI tabletop exercise with the Russian CTBT verification community. Exercise results are being used to help formulate U.S. policy for on-site inspections and may lead to international OSI exercises. In addition, Livermore scientists collaborate internationally in CTBT monitoring and seismic hazard mitigation activities. These activities contribute to U.S. efforts to develop seismic ground truth and promote confidence building in regions of national security interest.

The Laboratory's Culture—Scientific Excellence and Service to the Nation

Security and science are both central factors in the Laboratory's "culture." The staff at Livermore takes pride in their scientific and technical accomplishments. They are also attracted to the Laboratory and are motivated by the opportunity to serve the nation with the expectation that their work contributes to U.S. security. Our accomplishments require interactions with the broad scientific community, which if curtailed, will increase the difficulty and cost of science-based stockpile stewardship, greatly inhibit our contributions to nonproliferation, and damage the prospects of attracting new talent to sustain our important national security programs.

Our technical accomplishments also draw international attention to the Laboratory, including from foreign agents. Security is not just our business, it must be as much part of the way we operate as outside technical interactions. Security and openness are not incompatible objectives, but they require threat awareness, proper training, and vigilance. That balance is achievable. Few groups of people in the world are more painfully aware than Livermore employees what the loss of nuclear weapons secrets mean to the security of the nation. Few groups of people are more concerned about the impact of the diffusion of information on proliferation—vast amounts of technical information are in the open literature that can assist in nuclear weapons design and today's laptop computers are as powerful as the machines used to design weapons in the current stockpile. Finally, few have been more at the forefront of initiatives to limit the spread of weapons of mass destruction and to develop capabilities to prepare the nation to deal with the threat of their use.

CLOSING REMARKS

Accomplishing our mission depends crucially on science and technology interactions with the rest of the world. Simultaneously, we must ensure that the application of that science and technology to national security is protected at all levels. We have long recognized the inherent challenge involved in protecting national security information while fostering the interchange of ideas required for cutting-edge science and technology. Indeed, to a considerable degree, the nation's security rests on the technological advances that arise from the world-class R&D conducted at Livermore and the other national security laboratories.

A multi-faceted security apparatus is in place at our Laboratory, including physical security, operational security, personnel security, information security, communications security, cyber security, counterintelligence, and employee security awareness. We continually make adjustments and upgrades to address new threats and concerns. We take strong positive action on security and counterintelligence issues, whether they are anticipated or identified by us or by others, or are brought to our attention in the form of executive or departmental orders or inspections. Proactive and effective security and counterintelligence allows us to meet the challenge of ensuring national security while operating in a global world.